IN THE COURT OF APPEALS OF THE STATE OF IDAHO

Docket No. 35677/35684

STATE OF IDAHO,	)	**2009 Opinion No. 78**
	)	
Plaintiff-Respondent,	)	**Filed: December 28, 2009**
	)	
v.	)	**Stephen W. Kenyon, Clerk**
	)	
VINCENT ASCHINGER,	)	
	)	
Defendant-Appellant.	)	
	)	

Appeal from the District Court of the First Judicial District, State of Idaho, Kootenai County. Hon. John P. Luster, District Judge.

Order of the district court denying motion to suppress, affirmed; judgments of conviction, affirmed.

Molly J. Huskey, State Appellate Public Defender; Sarah E. Tompkins, Deputy Appellate Public Defender, Boise, for appellant.

Hon. Lawrence G. Wasden, Attorney General; Jessica M. Lorello, Deputy Attorney General, Boise, for respondent.

GRATTON, Judge

Vincent Patrick Aschinger, in these consolidated appeals, claims that the district court erred in denying his motion to suppress information obtained from a computer search and that his sentences are excessive. We affirm.

I.
FACTS AND PROCEDURAL BACKGROUND

Aschinger was charged with lewd conduct with a minor, Idaho Code § 18-1508, and ultimately entered an Alford[1] plea to an amended charge of felony injury to child, I.C. § 18-1501(1). The district court imposed a unified sentence of ten years with five years determinate. Aschinger was separately charged with video voyeurism, I.C. § 18-6609. The following facts are drawn from the evidence presented at the suppression hearing.

---

[1] *See North Carolina v. Alford*, 400 U.S. 25 (1970).

Aschinger and his former wife (Ms. Aschinger) owned a laptop computer during the time that Aschinger was being investigated on charges of lewd conduct. Aschinger purchased the computer for school while he and Ms. Aschinger were still married. Aschinger used the computer to store digital pictures taken of his and Ms. Aschinger's children. Aschinger downloaded the pictures through his user account. There were three user accounts on the computer, KID, KNA, and VPA. Ms. Aschinger testified that she had "free access" to the files on the computer. The Aschinger's children also had access to the computer as well as guests.

Approximately four months after Aschinger was charged with lewd conduct, and while he was incarcerated on that charge, Ms. Aschinger, while looking for pictures of their children on the computer, discovered several inappropriate pictures, including pictures of S.P. in her bathing suit as well as pornographic pictures of individuals she did not recognize. This discovery prompted her to take the computer to the police. Ms. Aschinger told Detective Dave Beck, one of the investigating officers, that the computer was her computer, but that both she and Aschinger had access to it. While at the police station, Ms. Aschinger turned on the computer and showed Detective Beck the pictures she had discovered of S.P. in her bathing suit with the focal point being on her genital area, breasts, and buttocks. Ms. Aschinger left the computer with Detective Beck and gave him permission to search it. Officer Mark Brantl conducted a search of the computer and, in addition to pornographic pictures and the pictures of S.P. in her bathing suit, found a movie file that depicted S.P. unclothed, changing into the same bathing suit. There were also still images made from the movie file. All of these files were located within the VPA user account. Based upon the evidence gathered during the search, Aschinger was charged with video voyeurism.

Aschinger filed a motion to suppress, which was denied. Aschinger entered a conditional guilty plea, reserving his right to appeal the denial of the motion to suppress. The district court imposed a determinate sentence of three years and ordered that it be served concurrently with the sentence in the consolidated lewd conduct case. Both sentences were ordered to run consecutively with a sentence imposed in an unrelated Latah County case. Aschinger now appeals.

II.

ANALYSIS

Aschinger contends that the district court erred in denying the motion to suppress. Aschinger argues that the files obtained from the computer were his personal files and that Ms. Aschinger did not have actual or apparent authority to consent to a police search of such files. He further asserts that the police search exceeded the scope of Ms. Aschinger's private search. In addition, Aschinger claims that the district court abused its discretion by imposing excessive sentences.

The standard of review of a suppression motion is bifurcated. When a decision on a motion to suppress is challenged, we accept the trial court's findings of fact that are supported by substantial evidence, but we freely review the application of constitutional principles to the facts as found. *State v. Atkinson*, 128 Idaho 559, 561, 916 P.2d 1284, 1286 (Ct. App. 1996). At a suppression hearing, the power to assess the credibility of witnesses, resolve factual conflicts, weigh evidence, and draw factual inferences is vested in the trial court. *State v. Valdez-Molina*, 127 Idaho 102, 106, 897 P.2d 993, 997 (1995); *State v. Schevers*, 132 Idaho 786, 789, 979 P.2d 659, 662 (Ct. App. 1999).

Aschinger first challenges the district court's determination that Aschinger did not have a reasonable expectation of privacy in the computer, which determination he argues was based upon an erroneous factual finding that the computer was in a "public space" and a misplaced reliance on *United States v. Barrows*, 481 F.3d 1246 (10th Cir. 2007). *Barrows*, as the district court recognized, addressed whether an employee had a reasonable expectation of privacy in a personal computer that was brought to work for work-related use and left in a public area without any password protection. *Id.* at 1248-49. Aschinger contends that the district court made an erroneous factual finding in stating:

> In this case, the defendant voluntarily moved his personal computer into a public space and took no measures to protect its contents from public inspection. Consequently, he did not enjoy a reasonable expectation of privacy, and in the officers' search there were no Fourth Amendment violations.

A careful reading of the context surrounding this statement, however, reveals that the district court was still referring to the facts in *Barrows*, not the facts in Aschinger's case. The district court prefaced its remarks by noting that *Barrows* was not "specifically on point," as it dealt with

"the expectation of privacy question." The court then gave a brief recitation of the facts of the case, including the above-quoted reference, and stated:

> Now, I realize that's not exactly on point, but I think it does make reference to some of the facts that have been provided here in terms of this computer, which, again, was part of the household and does not appear that there was any really substantial effort that had been undertaken to somehow necessarily preserve the privacy of any particular user account.

Therefore, Aschinger's contention that the district court made a factual finding that the computer was in a "public space" to support a determination that Aschinger did not have a reasonable expectation of privacy in the computer is belied by the record.

A. Third Party Consent and Authority

Aschinger's primary contention on appeal is that Ms. Aschinger did not have actual or apparent authority to consent to a search of Aschinger's private computer files and documents contained within his personal user account. While Aschinger acknowledges that Ms. Aschinger had overall access to the computer's hard drive, he argues that she did not have joint access to or control over personal information stored exclusively on Mr. Aschinger's user account. Thus, Aschinger contends that the search of the computer exceeded the scope of Ms. Aschinger's authority in violation of the Fourth Amendment of the United States Constitution.

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Fourth Amendment rights are implicated when police search things or places in which the defendant has a reasonable expectation of privacy. *Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990); *Oliver v. United States*, 466 U.S. 170, 177 (1984); *State v. Dominguez*, 137 Idaho 681, 683, 52 P.3d 325, 327 (Ct. App. 2002). Warrantless searches are per se unreasonable unless they come within one of the well-delineated exceptions to the warrant requirement. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-455 (1971); *Dominguez*, 137 Idaho at 683, 52 P.3d at 327. The State has the burden of showing that a warrantless search fell within one of these recognized exceptions to the warrant requirement or was otherwise reasonable under the circumstances. *State v. Reynolds*, 146 Idaho 466, 470, 197 P.3d 327, 331 (Ct. App. 2008). One such exception is voluntary consent to the search. *Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973); *State v. Stewart*, 145 Idaho 641, 644, 181 P.3d 1249, 1252 (Ct. App. 2008). The burden of proving that consent was voluntarily given rather than the result of duress or coercion, direct or implied, is on the State. *Schneckloth*,

412 U.S. at 222; *Bumper v. North Carolina*, 391 U.S. 543, 548 (1968). The voluntariness of consent is evaluated in light of all the circumstances. *Schneckloth*, 412 U.S. at 227; *State v. Huskey*, 106 Idaho 91, 94, 675 P.2d 351, 354 (Ct. App. 1984). Consent may be expressed through words, gestures, or other conduct. *State v. Fleenor*, 133 Idaho 552, 555, 989 P.2d 784, 787 (Ct. App. 1999). The consent need not be obtained from the defendant; it may be acquired from a third party with sufficient authority over the premises or item searched. *United States v. Matlock*, 415 U.S. 164, 171 (1974); *Dominguez*, 137 Idaho at 683, 52 P.3d at 327.

As an initial matter, we note that Aschinger does not argue that Ms. Aschinger's consent was not voluntarily given. Indeed, the record is devoid of any evidence of duress or coercion. Ms. Aschinger, upon discovering inappropriate pictures on the computer, telephoned the police and, of her own accord, took the computer to the police for further inspection. At the police station, Ms. Aschinger, with Detective Beck observing, turned on the computer, accessed several files, and then left the computer with the police and gave them permission to search it. Thus, it is clear that the consent was voluntary.

We must next determine whether Ms. Aschinger possessed authority to consent to the search of the computer. As noted above, a third party may consent to a search, thereby relieving the government of the warrant requirement, as long as such person possessed authority to consent. *Matlock*, 415 U.S. at 171; *Dominguez*, 137 Idaho at 683, 52 P.3d at 327. Actual authority exists if the third party shares with the defendant "common authority over or other sufficient relationship to the premises or effects sought to be inspected," *Matlock*, 415 U.S. at 171, as in the case of married couples or joint tenants. *State v. Brauch*, 133 Idaho 215, 219, 984 P.2d 703, 707 (1999); *Reynolds*, 146 Idaho at 473, 197 P.3d at 334. The United States Supreme Court has stated:

> Common authority is, of course, not to be implied from the mere property interest a third party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements . . . but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

Matlock, 415 U.S. at 171, n.7. A third party may alternatively be found to have apparent authority to consent to a search when an officer reasonably, even if erroneously, believes, based

on the totality of the circumstances known at the time, that the third party possessed authority to consent. *Georgia v. Randolph*, 547 U.S. 103, 109 (2006); *Illinois v. Rodriguez*, 497 U.S. 177, 186 (1990); *State v. McCaughey*, 127 Idaho 669, 674, 904 P.2d 939, 944 (1995); *Reynolds*, 146 Idaho at 473, 197 P.3d at 334. The reasonableness of a consent search "is in significant part a function of commonly held understanding about the authority that co-inhabitants may exercise in ways that affect each other's interests." *Randolph*, 547 U.S. at 111. This Court recently stated, "[e]ven a spouse may not have actual authority to consent to a search of property owned by the other if the spouse has no right or ability to control or access the item." *Reynolds*, 146 Idaho at 473, 197 P.3d at 334.

Actual authority of an individual to consent to the search of a personal computer, like other items and containers, is also based upon the individual's ability or right of control or access. An individual may have access or control of a computer, but not necessarily all of the information contained within the computer. This premise is the same as stated in *Reynolds* that "[c]ommon authority over shared premises does not necessarily translate into authority to search specific containers." *Id.*; *see also United States v. Karo*, 468 U.S. 705, 725-26 (1984) (O'Connor, J., concurring); *United States v. Salinas-Cano*, 959 F.2d 861, 865 (10th Cir. 1992). A joint owner or user may download or maintain individual files within the computer. If these files are accessible to the other joint user(s), then each can be said to have access and/or control of the files, as well as the computer itself. On the other hand, if an individual user takes precautions to ensure privacy and limit access and control over files, the joint user may not have sufficient access or control to consent to a search of those files. When assessing whether a third party has authority to consent to the search of a particular item which may contain other items, courts have examined, among other things, the nature of the item, any precautions taken to ensure privacy as to the item and its contents, and any visible markings which may signify privacy protections. *See United States v. Basinski*, 226 F.3d 829, 834-35 (7th Cir. 2000); *Salinas-Cano*, 959 F.2d at 865; *United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978). In the context of a computer, the authority of one user of a computer to consent to a search of another user's files may well depend upon the existence of password protection and/or encryption of files. As actual authority hinges on access or control, the presence of a password suggests potential limitations on a third party's access. Use of a password to limit general access to a computer or access to specific files is akin to locking one's file cabinet. For example, while a

file cabinet may be in the marital home and both spouses have general access to it, one spouse may have locked the bottom drawer and retained the only key. *See Reynolds*, 146 Idaho at 474, 197 P.3d at 335 (where locked box was located in room that defendant's wife seldom went into, wife still had at least apparent authority to consent to a search of the box because "she could readily access it by simply finding the correct key on a ring of keys located nearby"); *State v. Masten*, No. 5-88-7 (Ohio App. Sep. 29, 2009) (where file cabinet was located in home in a common area but defendant used it exclusively, kept it locked, and retained the keys, defendant's wife did not have authority to consent to a search of the file cabinet). Similarly, a joint user of a computer may have general access to several files on the shared computer, but may not have access to or control over other files that have password protection. Thus, generally, a joint user does not have "joint access or control," *Matlock*, 415 U.S. at 171, n.7, over another user's password-protected files unless that joint user has access to the password. *See Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (analogizing password-protected files to locked footlocker inside bedroom and concluding that where both defendant and his girlfriend had protected their personal files with passwords and girlfriend did not have access to defendant's passwords, girlfriend did not have authority to consent to a search of defendant's password-protected files); *United States v. Cole*, No. 8-CR-93-JAW (D.Me. July 24, 2008) (where defendant's life partner owned computer, had unrestricted access to computer, and had use of defendant's password, life partner had authority to consent to a search of computer, including defendant's files).

Where there is no affirmative intention and steps taken, however, to restrict co-users from accessing personal files through use of a password or other means, actual authority to consent to a search including those files may exist. *See United States v. Rader*, 65 M.J. 30 (C.A.A.F. 2007) (where roommate had unrestricted access to defendant's computer "for most purposes" and defendant had not made efforts to password protect or encrypt any files on computer, roommate had sufficient access to and control over computer to give valid consent to its search); *Antonelli v. Sherrow*, 246 Fed.Appx. 381, 384 (7th Cir. 2007) (where defendant had given his ex-wife his computer for duration of his incarceration, had not password-protected any files on computer, and had not indicated to her that any files were off-limits, his ex-wife could give valid consent); *United States v. Aaron*, 33 Fed.Appx. 180, 184 (6th Cir. 2002) (where record did not indicate that defendant's girlfriend could not access computer and defendant made no effort to protect his computer with a password, girlfriend had authority to consent to a search). Thus, where a

defendant has not taken affirmative action to password-protect personal files located on a shared computer, the defendant has "assumed the risk" that a co-user of the computer "might permit the common area to be searched." *See Matlock*, 415 U.S. at 171, n.7.

In this case, Aschinger argued before the district court, as he does on appeal, that because separate user accounts existed on the computer, Ms. Aschinger did not have authority to consent to a search of files located within the VPA (Aschinger's) user account. Aschinger contends that Ms. Aschinger did not have authority because she did not have joint access to or control over information stored exclusively in his user account. The district court found, however, that the evidence had not established that the computer "possessed any type of personal restrictions." The district court determined that Ms. Aschinger had "access and control and even arguably ownership over the computer." This determination is supported by Ms. Aschinger's testimony that she had "free access" to the computer and files and that she split use of the computer "50/50."

At the suppression hearing, Officer Brantl turned on the computer and noted that on the Windows display screen there were three usernames, KID, KNA, and VPA. Officer Brantl was able to click on the VPA username and testified that the computer's desktop came up "showing the files and everything on the desktop." This belies Aschinger's contention that Ms. Aschinger did not have joint access to and control over files stored within his user account. While a user account can be password protected, the mere existence of a user account without password protection does not necessarily signify an intention to limit another user's access to that user account. The district court specifically found that the demonstration indicated that "there were three user accounts and that one simply needed to click on one of the three user accounts to ascertain whatever information may be contained within that user account." The factual findings of the district court are supported by the record.[2]

Aschinger further maintains that because Ms. Aschinger did not make any attempt to access Aschinger's private information stored exclusively on his user account prior to finding the pictures, she did not have joint access to and control over that information. However, the fact

---

[2] Even if Aschinger had established that he had a password for his user account, the demonstration showed that his user account was still accessible. It is possible to format a user account to "remember" the password such that it becomes unnecessary to retype the password each time the user wants to access a user account. Formatting the user account in this way has the same effect as leaving the key to the file cabinet in the lock.

that Ms. Aschinger may not have previously accessed some files on the computer does not equate to a determination that those files were inaccessible to her. *See Aaron*, 33 Fed.Appx. at 184 (where defendant never told girlfriend that she could not use computer nor restricted her access with password protection, girlfriend's lack of use did not infer a lack of access). Furthermore, Ms. Aschinger testified that Aschinger always downloaded pictures of their children onto the computer through his user account. Contrary to Aschinger's assertion, Ms. Aschinger testified that when she wanted to view pictures of her children she would simply access them on the computer.

The district court also found that the computer had been left at the house and formatted such that it had availability to members of the household and guests. The district court determined, based upon Ms. Aschinger's testimony, as well as the demonstration performed by Officer Brantl, that no "substantial effort . . . had been undertaken to somehow necessarily preserve the privacy of any particular user account." The district court's findings are supported by the record. Based upon the record the district court correctly denied the motion to suppress.

Because Ms. Aschinger had actual authority to consent to a search of the computer and its files, we need not address whether she had apparent authority or whether the private search doctrine validated the search.

B. Sentencing

Sentencing is a matter for the trial court's discretion. Both our standard of review and the factors to be considered in evaluating the reasonableness of the sentence are well established and need not be repeated here. *See State v. Hernandez*, 121 Idaho 114, 117-18, 822 P.2d 1011, 1014-15 (Ct. App. 1991); *State v. Lopez*, 106 Idaho 447, 449-51, 680 P.2d 869, 871-73 (Ct. App. 1984); *State v. Toohill*, 103 Idaho 565, 568, 650 P.2d 707, 710 (Ct. App. 1982). When reviewing the length of a sentence, we consider the defendant's entire sentence. *State v. Oliver*, 144 Idaho 722, 726, 170 P.3d 387, 391 (2007). Applying these standards, and having reviewed the record in this case, we cannot say that the district court abused its discretion.

III.
CONCLUSION

Ms. Aschinger had actual authority to consent to the search of the computer and its files and the district court correctly denied Aschinger's motion to suppress. Aschinger has also failed

to show that the district court abused its sentencing discretion. Accordingly, Aschinger's judgments of conviction and sentences entered thereon are affirmed.

Judge GUTIERREZ and Judge MELANSON, **CONCUR.**